USAWC STRATEGY RESEARCH PROJECT

IS IT REALLY POSSIBLE TO PREVENT "INTERAGENCY INFORMATION-SHARING" FROM BECOMING AN OXYMORON?

by

Colonel Ronald R. Stimeare
United States Army

Dr. Jeffrey L. Groh
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **18 MAR 2005**	2. REPORT TYPE	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Is It Really Possible to Prevent**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Ronald Stimeare**	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**34**	

ABSTRACT

AUTHOR: Colonel Ronald R. Stimeare

TITLE: Is It Really Possible To Prevent “Interagency Information-Sharing” From Becoming An Oxymoron?

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 34 CLASSIFICATION: Unclassified

In July 2004, the “National Commission on Terrorist Attacks Upon the United States ” (9/11 Commission) issued its Final Report. As one of its 41 recommendations, the Commission proposed the creation of a National Counterterrorism Center (NCTC) in an attempt to resolve the interagency information sharing challenges. The Director of the NCTC would be appointed by the President with the advice and consent of the Senate, and would report to the Commission’s proposed new National Intelligence Director. On December 17, 2004, the President signed into law an Intelligence Reform Bill, which formally established the NCTC. In order for the NCTC to achieve a successful interagency information sharing solution however, it must first develop a holistic enterprise solution, which creates a synergistic effect between people, processes and technology.

The greatest mistake the United States can make is to allow itself to believe a quick organization change and a few technical solutions are going to resolve the Interagency Information-Sharing (IIS) conundrum. Instead a methodical approach must first be taken to obtain clarity regarding the IIS deficiencies that led up to the 9/11 catastrophe, as well as the mission of the new NCTC. Second, Knowledge Management (KM) as a concept needs to be used to achieve ISS success. This includes addressing the challenges of affecting change with the intelligence culture and its people. Third, the construct and processes of KM implementation needs to be accelerated by taking the best practices of DOD and tailoring them to the NCTC mission. Next, the NCTC needs to implement enterprise resource planning to ensure rapid information exchange with the goal of achieving total knowledge dominance over our adversaries. Finally, we must fuse all of this together into a synergistic solution, in order to produce an organization that can successfully bridge the interagency information-sharing divide and thus prevent “interagency information-sharing” from becoming an oxymoron.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I owe great thanks to my Project Advisor, Dr. Jeffrey Groh for his advice, guidance, and insights. His expertise in Knowledge Management has assisted me greatly in the writing of this paper.

I would like to thank my Faculty Instructor, Dr. Louis Nigro for his ability to take something complex and make it understandable in just “three-simple-steps”.

I would also like to thank my parents for encouraging me through my life’s journey.

Finally, I would especially like to thank my wife Geri; son Scott; and daughter Melissa. Without their continuous support throughout my military career, I would not have been able to do so much in such a short space of time.

IS IT REALLY POSSIBLE TO PREVENT "INTERAGENCY INFORMATION-SHARING" FROM BECOMING AN OXYMORON?

In July 2004, the "National Commission on Terrorist Attacks Upon the United States " (9/11 Commission) issued its Final Report. As one of its 41 recommendations, the Commission proposed the creation of a National Counterterrorism Center (NCTC) in an attempt to resolve the interagency information sharing challenges. The Director of the NCTC would be appointed by the President with the advice and consent of the Senate, and would report to the Commission's proposed new National Intelligence Director. On December 17, 2004, the President signed into law an Intelligence Reform Bill, which formally established the NCTC. In order for the NCTC to achieve a successful interagency information sharing solution however, it must first develop a holistic enterprise solution, which creates a synergistic effect between people, processes and technology.

The greatest mistake the United States can now make is to allow itself to believe a quick organization change and a few technical solutions are going to resolve the Interagency Information-Sharing (IIS) conundrum. Instead a methodical approach must first be taken to obtain clarity regarding the IIS deficiencies that led up to the 9/11 catastrophe, as well as the mission of the new NCTC. Second, Knowledge Management (KM) as a concept needs to be used to achieve ISS success. Third, the construct and processes of KM implementation needs to be accelerated by taking the best practices of DOD and tailoring them to the NCTC mission. Next, the NCTC needs to implement enterprise resource planning to ensure rapid information exchange with the goal of achieving total knowledge dominance over our adversaries. Finally, we must fuse this into a synergistic solution, in order to produce an organization that can successfully bridge the interagency information-sharing divide and thus prevent "interagency information-sharing" from becoming an oxymoron.

DEFICIENCIES IDENTIFIED BY THE 9/11 COMMISSION REPORT

On September 11, 2001 the United States suffered a horrific attack at the hands of terrorists, which left many in shock and many more still, asking themselves why, as the world's most powerful nation, were we not better prepared? Following the tragedy, a 10-member National Commission, released a 585-page final report that probed the federal government's failures leading up to the September terrorist attacks. In the report, the commission stated, "Our intelligence and law enforcement agencies did not manage or share information or effectively follow leads to keep pace with a very nimble enemy".[1] The report probed deeply into the cause and effects of intelligence hording and concluded the biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systematic resistance to sharing information.[2]

The 9/11 Commission Report cites numerous examples of information sharing deficiencies. Members highlight problems with orders not getting to the right people, and a lack of effective information sharing. The report discusses how the Central Intelligence Agency (CIA) has no real control over Department of Defense's (DOD) intelligence capabilities. Yet the CIA Director is supposed to oversee all intelligence services.[3] Essentially, he has been given all of the responsibility, but none of the authority in which to effectively influence policy, procedures or budgetary allocation across the intelligence community. The report discusses how the Immigration and Naturalization Service (INS) was left out of the loop in information sharing at critical times. It further points out, had there been effective communications between the Federal Bureau of Investigation (FBI) and the CIA, Khalid Al-Mihdhar (one of six participants known as the organizers of the 9/11 attacks and suspected of having been involved with the bombing of the USS Cole) would have been captured in New York, two days after an FBI-CIA meeting.[4] The report highlights massive breakdowns and overburdening of existing communications systems and discusses once again, the lack of management operations and teamwork in the intelligence arena and emphasizes the urgent need to pool resources and the need to develop economies of information.[5] These are but a few examples of the multitude of interagency information sharing deficiencies and impediments that existed prior to 9/11. Unfortunately, many deficiencies still exist between the various intelligence and antiterrorist organizations.[6]

As a result of the 9/11 Commission's exposure of these blatant and unforgivable lapses in interagency information sharing, intelligence reform is starting to gain momentum at an unprecedented pace. In addition to his establishment of the NCTC,[7] in September 2004, the President appointed Peter Goss as the new CIA Director. On October 7, 2004 the U.S. Senate passed a bill that will create a National Intelligence Director (NID) post to coordinate the work and budgets of related agencies[8] and on December 17, 2004 the President signed that bill into law. Last year, the 2003 budget proposed an increase in spending of $722 million on programs that will use information technology to more effectively share information and intelligence horizontally (among federal agencies) and vertically (between federal, state, and local governments).[9] With the implementation of the 9/11 Commission's highest recommendations, the stage is now set to allow an organization such as the NCTC to become a key enabler towards achieving interagency information-sharing.

NATIONAL COUNTERTERRORIST CENTER

When the President established the National Counterterrorist Center (NCTC) in August 2004, he specified that the CIA Director would initially have supervisory responsibilities over the center. This allowed for the expedient establishment of the center within an existing mature organization with deep resources and addressed the interagency information sharing challenges of the past. He gave the organization the explicit authority and responsibility to ensure the shortfalls of the past were now corrected. He ordered the NCTC to serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism.[10] He authorized the Center to receive, retain and disseminate information from any Federal, State, or local government, or other source necessary to fulfill its responsibilities, and clearly articulated that agencies authorized to conduct counterterrorism activities may query the Center's data for any information to assist in their respective responsibilities.[11]

The NCTC is further charged with conducting strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies.[12] It is assigned operational responsibilities to lead agencies for counterterrorism activities that are consistent with applicable law and that support strategic plans to counter terrorism.[13] The NCTC will serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support; it will ensure agencies have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis.[14]

To address the compartmentalizing and security complaints of the past, the President ordered them to produce reports on terrorism information with contents and formats that will permit dissemination that maximizes the utility of the information in protecting the territory, people, and interests of the United States.[15] In order to ensure there is no ambiguity to what information needs to be reported and shared, the President defines the term "Terror Information" with such specificity, as not to leave it up to individual organizations for interpretation.

This executive order leaves no doubt to what the President is expecting of the NCTC and supporting agencies. The challenge is getting the people to do what is now demanded of them, as well as putting the enabling processes and technology in place. A methodology in which to do this already exists in the corporate world. It is found within the concept of Knowledge Management.

USING KNOWLEDGE MANAGEMENT (KM) AS A CONCEPT FOR ACHIEVING INTERAGENCY INFORMATION SHARING SUCCESS

Knowledge Management (KM) is a deliberate, systematic business optimization strategy that selects, distills, stores, organizes, packages and communicates information essential to the business of a company or organization in a manner that improves employee performance and corporate competitiveness.[16]

The NCTC, through connectivity, access to and exchange of valid information, and the expertise and judgment of people with the right knowledge at the right time to share where and as needed, will be able to stay alert and watchful 24/7 in defense of our country. If properly implemented, the operators within the NCTC will be living and working in an organization committed to ubiquitous communications and invisible technology, where through information sharing and organizational learning built on trust and respect, people at all levels will be able to make and implement efficient and agile decisions.[17]

To achieve all of this however, it is imperative to understand the intelligence information-sharing community, to include its culture, people, and organization as well as the KM processes and technologies which need to be leveraged, in order to establish an organization that is initially postured for success at its inauguration.

CULTURE

Culture is a multidimensional enigma that envelops an organization.[18] Every member of an organization contributes to the culture in some manner. The history, style of leadership, structural stability, level of workforce empowerment and the ability to adapt to a changing environment all contribute to the culture of an organization.[19] Today's intelligence community largely untouched since its creation stemming from the National Security Act of 1947, is structurally unsound in the information age.[20] America's intelligence agencies have been resistant to shed the Cold War mentalities for which they were originally created, and endless battles over funds and turf have hampered agencies' overall cooperation and effectiveness.[21] The need to protect sources and methods at virtually any cost, as well as the need to minimize any risk of leaks, is critical to the community's very existence. This same need to protect information is also a restraint to sharing.[22]

There are many other cultural factors that inhibit knowledge transfer among agencies as well. They are called inhibitors or "frictions" because they slow or prevent transfer and are likely to erode some of the knowledge as it tries to move through or across intelligence organizations.[23] These include: lack of trust; differences in cultures, vocabularies, frames of reference; lack of time and meeting places, narrow ideas of productive work; status and rewards only going to knowledge owners; lack of absorptive capacity in recipients; belief that knowledge is the prerogative of particular groups, “not-invented-here syndrome”; along with intolerance for mistakes or need for help.[24] To overcome these cultural challenges within the NCTC as well as the overall intelligence community, a serious commitment to Change Management (CM) will be required.

Understanding the culture of the intelligence community is essential to bringing about change. Just as important however, is understanding who the key people are and how an organization can be structured in order to gain efficiencies, which in turn can ensure rapid change.

PEOPLE AND ORGANIZATION

The people within the new NCTC are no different than those in many other organizations. They consist of upper and mid-level management, as well as the various groupings of employees. These include plans and policies, research, legal, public affairs, resource management, budget, administration and automation support. In addition, they will most likely be establishing a rather large operations section consisting of current operations, future operations along with a crisis action cell. In order for the organization to be effective however, the NCTC cannot allow itself to be organized into a bureaucratic rubrics cube, which encourages overly compartmented, stovepipe management and reporting. The physical and virtual walls must never be built within this new organization. Instead it must have open lines of communication and the ability to rapidly share information internally, externally, horizontally as well as vertically. The key to achieving this goal is trust.

Understanding the culture, people, and how to organize smartly will allow the doors to the corridor of change, to be swung wide-open. At this point it is imperative to fully understand how knowledge management (as a process) can assist in the journey to interagency information sharing utopia and develop the standardized processes in which to give stability and focus amongst the various departments and members of the NCTC.

PROCESS

As knowledge management continues to mature and evolve, it is clear that real success does not come from simply grafting knowledge activities onto existing work processes.[25] Instead, the knowledge management process has to be mixed and “baked” into key knowledge work processes.[26] How the NCTC will create, gather, store, share, and apply knowledge must blend well with how the intelligence community analyst, operators, researchers and managers work on a daily basis.

It will be important to build explicit linkages between knowledge management and the knowledge work process it is designed to support, both within the NCTC and to the various organizations across the intelligence community. The linkages should specify how knowledge should be imported to and exported from the process, when and how in the process this knowledge should be used, and what difference it should make in the outcome.[27]

As the new NCTC is established, it will be important to ensure these linkages are established with a clear understanding of the National Counterterrorism Center's mission, culture, people, organization and available technology.

TECHNOLOGY

It is now common to observe that although the phenomenon of management attention upon KM was given birth, to a large degree, by the appearance of the Internet and its brethren, intranets and extranets, fundamentally KM is more about people and corporate/organizational culture than it is about technology. [28] Those that have been led down the path of a quick technological solution have most often and regrettably failed.[29] The designers of the KM solution for the NCTC will need to provide loose pairing between technology and business architectures so that existing technology infrastructure does not straightjacket the evolution of the business model.[30] Greater technological integration will help to achieve more efficient optimization for knowledge harvesting. However, there will be a critical need for ensuring rapid adaptation of the business performance outcomes to the dynamic shifts in the business environment while keeping them loosely coupled with prespecified technology architectures.[31] The new paradigm of flexible, adaptive, and scalable systems will accommodate real-time changes in information and data across the business ecosystems network.[32] It is essential to tie not only technology, but processes, people, organization and culture together in order to achieve a viable information sharing solution, a solid construct is required.

LEVERAGING DOD'S ARMY KNOWLEDGE MANAGEMENT (AKM) PROCESS AS A CONSTRUCT FOR INTERAGENCY INFORMATION SHARING IMPLEMENTATION

Today's business environment is characterized by radical change. Such a volatile climate demands a new attitude and approach within organizations—actions must be anticipatory, adaptive, and based on a faster cycle of knowledge creation.[33] Secretary Rumsfeld echoed these same ideas in an article in the May/June 2002 issue of *Foreign Affairs*: "Preparing for the future will require new ways of thinking, and the development of forces and capabilities that can adapt quickly to new challenges and unexpected circumstances. The ability to adapt will be critical in a world defined by surprise and uncertainty." [34] Mastering adaptability is essential if we wish to achieve information, knowledge and decision superiority both on and off of the battlefield.

The concept of Knowledge Management attempts to secure the learning experiences, as well as the work products, of the individuals who comprise an organization.[35] This concept is not new. In 1995, Ken Derr, then CEO of Chevron, stated: "managing knowledge is something all companies will have to master if they expect to compete in the global economy. Those that can learn quickly and then leverage and use that knowledge within the company will have a big advantage over those that can't. This will be true whether knowledge is developed internally or acquired elsewhere".[36] Even with this realization, and the maturing theory of Knowledge Management (KM), the business world has often failed miserably in its implementation of information sharing. As of this year, only 37% of corporations have a knowledge strategy now, down from 50% in 2001. This is partially a result of trying to implement it solely as a technical solution (a box with a few wires) and not getting people involved early on.[37]

Fortunately, the Department of the Army, G6/CIO has painstakingly written a comprehensive Strategic Plan for Army Knowledge Management (AKM). This plan recognizes that becoming a knowledge-based organization involves more than technologies – it requires deep cultural shifts – from traditional practices to collaboration, teamwork and innovation; from information sharing to knowledge sharing; from stovepipe to enterprise processes; and from traditional skills to Internet-Age competencies.[38]

Leadership and trust are at the heart of Army Knowledge Management. With the creation of the newly formed NCTC, the intelligence community has the opportunity to ensure the right people are in place to make KM a success. The Army's construct can be applied to the NCTC's quest for improved Interagency Information Sharing as a framework in which to quickly build upon. In so doing, it will greatly accelerate the implementation of a Knowledge-based solution. This then has the potential to become the standard across the United States intelligence community with worldwide implications.

The Department of Defense strongly believes Knowledge Management (KM) is a key contributor to achieving Information Superiority (IS) which is a key enabler to achieving Decision Superiority (DS).[39] In their mind, Decision Superiority is the process that enables you to make decisions better and faster than an adversary – it is essential to executing a strategy based on speed and flexibility[40]. Decision superiority requires new ways of thinking about acquiring, integrating, using and sharing information. It necessitates new ideas for developing architectures for command, control and communications and computers (C4) as well as the intelligence, surveillance and reconnaissance (ISR) assets that provide knowledge of adversaries.[41]

Decision Superiority requires precise information of enemy and friendly dispositions, capabilities, and activities, as well as other data relevant to successful campaigns.[42] Battlespace awareness, combined with responsive command and control systems, supports dynamic decision-making and turns information superiority into a competitive advantage adversaries cannot match.[43] Both the NCTC and the intelligence community can similarly achieve these same goals as long as each organization is willing to commit and implement continuous change.

As people integrate the technology into their daily work routines, they will find it easier and more rewarding to share their experiences and insights with others. This way, people develop a culture that not only sustains knowledge management, but also nurtures it.[44] The AKM strategic plan was developed to be applicable across the entire Army Enterprise: Active Army, DA Civilians, Army Reserves, and National Guard, during both peace and war. Its goals are to be achieved at all levels across the enterprise, with an emphasis on standardized, enterprise-level mission and business practices.[45] As will become quickly apparent, it is a construct that is very applicable to the intelligence community, especially the NCTC.

Most important to this solution, are the guiding thirteen principles for AKM. They are the underlying tenants upon which the Army is building and institutionalizing its Knowledge Management program.[46] Without a solid and standardized foundation, any huge endeavor such as this one by the intelligence community would be doomed to eventual failure.

First, business rules, processes and information across the enterprise must be standardized.[47] This is especially true when the NCTC is dealing with over 55 other intelligence agencies on a daily basis. At this year's 3rd Annual Peacekeeping Intelligence Conference which was held in Stockholm, Sweden 2-3 December 2004, Larry Sequist presented his thoughts on how important it is to think even beyond just the immediate intelligence community, and ensure information is being openly shared across all of the seven information "tribes". These are National, Military, Law Enforcement, Business, Academic, NGO & Media, and Religious & Clans.[48] By broadening standards across each of the tribes, information-sharing at all international levels can be capitalized.

Second, unnecessary duplication, incompatibility and redundancy of data, systems and business practices must be eliminated.[49] The President's Directive highlights this as the primary goal of the NCTC, thus giving them both the responsibility and authority to ensure compliance. To be successful however, Change Management (CM) is required. Comprehensive change management requires a three-phase approach that takes human dynamics and human needs into account.[50] Each type of organizational culture needs all three phases to institute a successful change management plan. Within the NCTC, not all members will be permanently assigned or organic to the center. Some will be liaisons sent from their parent organizations. Therefore buy-in from those organizations will have to be done up front, in order for true change to be realized. The three phases must include education, training and promotion.

Education is essential to ensure the theory behind the interagency information sharing vision is clear. This way the "why" questions can be answered with sound reasoning to build a foundation of understanding throughout not only the NCTC, but the entire intelligence community as well.[51]

Once the processes and technology are established, training must allow the members of the NCTC to experience the new information-sharing environment in a "lab" setting where clarifying questions can be asked and issues addressed prior to integrating the new behavior into the everyday work routines.[52] New human behaviors and paradigm shifting practices will be instituted; therefore, the organization must provide the necessary support to ensure success.[53] Upfront reassurance; positive reinforcement and consistent demonstrations of success will greatly expedite the learning and implementation process.

Also key is the promotion of the KM concept. The future interagency information sharing environment and benefits must be clearly articulated and envisioned by all members of the NCTC. This must begin with the leadership. Through positive role modeling, others will soon follow. A steady barrage of encouragement and motivation to subordinates will expedite success. After the education and training phases are complete and the new behaviors are in place on a day-to-day basis, various and creative incentives must be offered to encourage positive reinforcement over an already negative and distrustful cultural environment.[54] Only through an eventual CM cultural change will we see unnecessary duplication, incompatibility and redundancy of data, systems and business practices permanently eliminated.

Third, information must be captured and validated only once, and then reused across the enterprise.[55] This will ensure burden sharing and division of labor occurs in order to achieve presidential directed efficiencies.

Fourth, reuse what they have, before buying or building new.[56] This will force the NCTC to assess available assets and develop processes and equipment solutions based on best practices and appropriate technology. If not done correctly, the NCTC may move out too quickly, and find itself in a similar situation as the FBI. In January 2005, the FBI acknowledged that it might have to scrap a new 1.7 million dollar computer program aimed at helping agents share information in the war on terror because officials now consider it inadequate and outdated due to it taking over four years to implement.[57] These problems will most likely contribute to the overall delay of a $500 million overhaul of the FBI's antiquated computer system.[58]

Fifth, place greater emphasis on cooperative strategies for satisfying the common needs of soldiers and civilians across the enterprise.[59] A "Partnership" model, embraced by both the previous Clinton Administration and the Bush Administration, is potentially very responsive and adaptable, it leverages both public and private sector strengths, and takes into account that 85% of U.S. critical infrastructures are owned or operated by the private sector.[60]

Sixth, enable and accelerate sound decision-making through architecture-based analysis and evaluation.[61] In order to analyze, evaluate and manage knowledge, one must first be able to categorize it. The most common approach is to simply be able to distinguish between explicit and tacit knowledge. Explicit knowledge refers to knowledge that can be easily articulated in words, pictures and formulae, whereas tacit knowledge refers to knowledge entrenched in the minds of the knower, such as insights, hunches and judgment.[62] Once this is understood, the means in which to achieve this knowledge can be more effectively designed and executed.

Seventh, ensure security and protection of sensitive information.[63] In the intelligence world this is paramount. The 9/11 Report gave several examples in which information can be shared, but still protect the source of the information. Additionally, this can be accomplished by using trusted networks, acceptable procedures and technology such as biometrics for auditing and authentication.

Eighth, reduce the total cost of Information Technology / Information Management (IT/IM).[64] With Congress's approval of both the NID and NCTC, they are now able to design, purchase and implement enterprise solutions across the entire intelligence community, which has the potential of drastically reducing costs normally associated with training, maintenance, life cycle management and sustainment.

Ninth, use continuous improvement and evolutionary transformation.[65] Similar to how Secretary of Defense Rumsfeld has been able to influence transformation and reorganize units within the military; the new National Intelligence Director (NID) will have a similar opportunity to affect change within both the NCTC and intelligence world.

The NID must ensure the NCTC is able to organize itself smartly. It is imperative they have representatives (Liaison Officers/LNOs) from each of the key organizations and intelligence agencies in which information must openly flow. At the very least, these need to include Department of Defense (DOD), Department of State (DOS), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Law Enforcement, Treasury, Homeland Security, Immigration, Customs, Transportation and Department of Justice. In addition, international agencies also need to be considered. Mirror Operation Centers need to exist at the parent LNO organizations to ensure fluid information exchange. Fusion Cells need to be a component of each operation center and the function and responsibility of Knowledge Management needs to reside in each.

As stated in the 911 Report: "The culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information—to repay the taxpayers' investment by making the information available." Decentralized fusion cells will act as the "trusted" traffic cops for information flow when problems arise between organizations, thus formalizing and expediting the process and allowing continuous improvement and evolutionary transformation to occur.

Tenth, integrate performance management in every decision process.[66] Measuring and being able to accurately articulate success will be paramount to continued success. Technical measures must be balanced with business measures, and managers of the NCTC must continually work to establish active feedback between performance measures and business processes.[67]

Eleventh, post before processing.[68] This processing method allows items to be properly critiqued and reviewed for accuracy prior to distributing or placing in a repository. Levels of reliability and applicability must be relatively obvious. Usefulness becomes critical when dealing with massive amounts of data and information.

Twelfth, everyone is a "teacher", everyone is a "learner".[69] Knowledge Management is not an end state, but rather a journey. As such, change is inevitable. Only by learning will people be able to quickly change and take advantage of new methods of sharing information along with leveraging the technology that will make those changing methods possible. As a result of information sharing being such a large and sometimes overburdening endeavor, the more decentralized and personalized the process of managing, posting and obtaining the information becomes, the more successful knowledge management will become. Therefore, every individual must be proficient in each of these aspects to add value to the overall synergistic effect of KM.

And lastly, every human interaction is viewed as an opportunity to acquire and share knowledge.[70] In the intelligence world, Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT), Open Source Intelligence (OSINT) and Technical Intelligence (TECHINT) are all important, however Human Intelligence (HUMIT) is clearly recognized as a critical source of gaining information that has no equivalent. Being able to quickly distribute this information to the necessary agencies in a timely manner will be the challenge, which the NCTC can help facilitate.

The methodology the Army has adopted to achieve knowledge superiority is through the achievement of five major goals. In the case of the NCTC, these goals can be executed in sequential steps. The initial step is to integrate knowledge management concepts and best practices to promote the knowledge-based force. This is followed by the adoption of governance and implementation of cultural changes in order to become a knowledge-based organization. Next, the NCTC can harness human capitol for the knowledge-based organizations, followed by institutionalizing an Army-Like: Army Knowledge Online (AKO) as the enterprise portal to provide universal, secure access for the entire organization. Lastly, the NCTC must manage the information structure as an enterprise to enhance capabilities and efficiencies.[71]

Technology alone will never solve the overall information-sharing problem between agencies. However, once the NCTC is fully established and once a KM framework and best practices have been firmly implemented, then technology is capable of taking the interagency intelligence community to higher levels of excellence, very few thought originally possible.

TECHNOLOGY

There are currently five categories of technology tools that can be used to support knowledge management activities within the NCTC and across the intelligence community. They are learning tools, content tools, discovery tools, relationship tools and collaboration tools.[72] The learning tools and the content tools support the transfer of knowledge and the building of a repository. The discovery tools are used to generate new knowledge from mounds of existing data, and thus they support knowledge creation.[73] The relationship tools support decisions in business processes by uncovering the preferences and needs of consumers, agents and organizations. Hence, they are used to create, transfer and build repositories of knowledge.[74] The last category is collaborative tools. These are essential in enabling a collaborative KM environment in which participants share data, information, knowledge, perceptions, ideas, and concepts.[75] The classic military example of collaborative planning, using various tools, is where actors with different functional and geographic areas of responsibility focus their attention on achieving assigned missions. Their goals are to create a common (shared) understanding of the situation; take advantage of their differential knowledge, expertise, information and capabilities; and organize the activities they control in time and space such that they will avoid mutual interference and have a synergistic effect. In other words, they want to plan so their actions will be synchronized.[76]

Many technology tools that are available today have the capability to allow us to work in an environment from unclassified through top-secret levels, as well as with multinational partners. Today's collaborative tools allow us to do both voice and text chat and share a common operational view amongst those participating in the collaborative session. Advanced White Boarding is now commonplace, as well as multiple virtual workspaces.[77]

The Joint Forces Command is making great strides in the collaborative field. They are currently looking at establishing a Virtual Information Warehouse. It's a conceptual initiative that aims at establishing a primary repository for information and knowledge products necessary for joint operations in a collaborative environment.[78] The technology will allow access to information, which will be available in or through the "warehouse" and transparent to the user.[79]

Joint military doctrine has stated a Common Operating Picture (COP) is important to collaboration and an essential contributor to shared situational awareness and understanding. It is a single identical display of relevant information shared by multiple users, organizations and commands across an entire theater.[80] The applicability of this concept within the NCTC is enormous, especially when trying to coordinate and synchronize interagency and multinational intelligence efforts.

The Army is continuing to move towards a Web-based Enterprise Portal. This portal (electronic gateway) currently functions as an individual user's personalized point of entry to information, accessible either over their local network or global network. It has the potential to link into their virtual warehouse, once the concept fully matures.[81] Newer generations of portals are starting to include collaborative tools such as instant messaging, audio and video-conferencing, shared calendaring and document sharing.[82]

While search and information retrieval has made real advances in the past decade, most searchers simply cannot review scores of returned search results and manually cull them for useful knowledge. Even when dealing with the most highly relevant results, result sets can quickly number into the hundreds or thousands, rapidly outstripping human capacity to process and absorb them.[83]

Recent advances in this field have focused on using taxonomies to categorize or organize information into meaningful frameworks that reduce information overload and add some logical structure that humans can rapidly navigate to find high concentrations of topic-specific, related information.[84] Taxonomies are flexible structures, as they can be developed to cover many different topics to any desired level of granularity. Many standards or industry-accepted taxonomies are becoming readily available and key search and classification vendors are making good use of taxonomies, thus provoking an information retrieval paradigm-shift long understood by library scientists.[85]

And lastly, just over the horizon there is the emergence of a new combination of information architectures, which need to be accelerated in order to join the fight against Global War on Terror. These are the newly developed intelligent networks, semantic web and synthetic information architectures, along with federated super-sized data systems. The semantic web alone will give us the ability to use Extended Markup Language (XML) and web ontology language to quickly gain meaning from the web. The idea will be to gain more context from the web rather than just scores of information and data. These emerging technologies, along with the tools previously discussed, will finally make it possible to provide real-time access to distributed data while protecting privacy and providing full security controls to the owners of each discreet data element.[86]

CONCLUSION

Once clarity is obtained regarding the Interagency Information Sharing (ISS) deficiencies that led up to the 9/11 catastrophe, as well as the mission of the new NCTC, Knowledge Management as a concept needs to be used to achieve ISS success. Cultural changes must be achieved through education, training and promotion. The NCTC must organize itself for success if it hopes to become an information-sharing key enabler in support of the Global War on Terrorism. It is imperative they have representatives (liaison officers) from each of the key organizations and intelligence agencies. The NCTC must be able to effectively coordinate with each of the seven international and domestic “Information tribes”. Mirror Operation Centers, Fusion Cells with KM responsibilities need to exist at those Organizations to ensure fluid information exchange. Trusted networks need to be established along with agreed procedures and biometrics for auditing and authentication. The intent should be to become a Virtual Intelligence Organization, not fragmented agencies with gapping seams, which only on occasion, pass snippets of information to keep each other temporarily satisfied.

The construct and processes of KM needs to be implemented by taking the best practices of DOD and tailoring them to the NCTC mission. Enterprise technical solutions must be applied to ensure rapid information exchange with the goal of achieving total knowledge and information dominance over our adversaries. An initial practical solution can include an integrated KM portal, knowledge repository (content management), and expertise Location Management (yellow pages – find out who knows what), linked to an integrated groupware framework (collaboration tool). As trust, time and dollars increase, additional technological solutions as previously discussed, can be systematically inserted within the NCTC and across the intelligence and information community in an efficient and effective enterprise manner.

The greatest mistake the United States can make is to allow itself to believe the establishment of a new organization such as the NCTC along with implementing a few technical solutions under the guise of Knowledge Management is going to resolve the interagency information-sharing conundrum. Only by implementing a holistic enterprise solution, which creates a synergistic effect between people, processes and technology can a successful interagency information sharing solution be realized and thus prevent “interagency information-sharing” from becoming an oxymoron.

WORD COUNT=5908

ENDNOTES

[1] Dibya Sarkar, “9/11 Report Urges Info Sharing, Biometrics,” 20 September 2004; available from <http://www.fcw.com/fcw/articles/2004/0719/web-911-07-22-04.asp>; Internet; accessed 20 September 2004.

[2] The 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: U.S. Government Printing Office, 2004), 416.

[3] Charles Reimer Mr HQDA DCS G-3/5/7 <charles.reimer@us.army.mil> “9-11 Commission Report,” electronic mail message to William T. Johnsen, Ph.D <William.Johnsen@carlisle.army.mil>, 24 September 2004.

[4] Ibid.

[5] Ibid.

[6] Joe Fiorill, “Panel Seeks Broad Terrorism Information-Sharing Changes,” 13 December 2004; available from <http:// www.govexec.com/dailyfed/1204/121304gsn1.htm>; Internet; accessed 17 December 2004.

[7] George W. Bush, “Executive Order National Counterterrorism Center,” 27 August 2004; available from <http://www.whitehouse.gov/new/releases/2004/08/20040827-5.html>; Internet; accessed 8 October 2004.

[8] Andrea Seabrook, “Senate Approves U.S. Intelligence Overhaul,” 7 October 2004; available from <http://www.npr.org/templates/story/story.php?storyld=4074833>; Internet; accessed 8 October 2004.

[9] George W. Bush, *National Strategy for Homeland Security* (Washington, D.C.: The White House, July 2002), 68.

[10] Bush, “Executive Order National Counterterrorism Center.”

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Bryan Bergeron, *Essentials of Knowledge Management* (Hoboken: John Wiley & Sons, 2003), 8.

[17] Michael E.D. Koenig and T. Kanti Srikantaiah, eds., *Knowledge Management, Lessons Learned, What Works and What Doesn’t* (Medford, NJ: ASSIS&T, 2004), 281.

[18] Maribeth Achterberg, “How Culture Affects Information Sharing in an Organization,” 30 November 2001; available from <http://www.kwork.org/White_Papers/cultural.html>; Internet; accessed 12 November 2004.

[19] Ibid.

[20] James T. Lewis, “Reform by Catastrophe: How the Department of Homeland Security Fails America’s Need for Real Intelligence Reform,” November 2004; available from <http://www.american.edu/sis/students/sword/back_issues/7.pdf>; Internet; accessed 19 December 2004.

[21] Ibid.

[22] Juris Kelley, “Overcoming information Sharing Obstacles and Complexity,” November 2003; available from <http://www.chm.net/docimg/wp_overcoming.pdf>; Internet; accessed 12 November 2004.

[23] Thomas H. Davenport and Laurence Prusak. *Working Knowledge: How Organizations Manage What They Know* (Boston, MA: Harvard Business School Press, 2000), 96.

[24] Ibid., 97.

[25] Ibid., x.

[26] Ibid., xi.

[27] Ibid.

[28] Koenig, 487.

[29] Mei Fong, “Mind over Matter,” *Far Eastern Economic Review* (29 July 2004,167, Iss. 30): 39 [database on-line]; available from ProQuest; accessed 21 September 2004.

[30] Koenig. 100.

[31] Ibid.

[32] Ibid.

[33] Office of the Secretary of Defense, Comptroller, “Knowledge Management,” 21 September 2004; available from <http://www.defenselink.mil/comptroller/icenter/learn/knowledgeman.htm>; Internet; accessed 21 September 2004.

[34] Lewis.

[35] Office of the Secretary of Defense, Comptroller.

[36] Melissie Clemmons Rumizen, *The Complete Idiot’s Guide to Knowledge Management* (Madison, WI: CWL Publishing Enterprises, 2002), 1.

[37] Fong.

[38] Chief Information Office, United States Army, *The Army Knowledge Management Strategic Plan*, 2nd ed. 8 June 2003 (Washington, D.C.: U.S. Government Printing Office, 2003), ii.

[39] Richard B. Myers, *National Military Strategy of the United States of America 2004* (Washington, D.C.: U.S. Government Printing Office, 2004), 17.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Chief Information Office, 2.

[45] Ibid.

[46] Ibid., 3.

[47] Ibid.

[48] Larry Sequist, "Information Peacekeeping & Collective Intelligence," 3 December 2004; available from <http://www.oss.net/extra/news/?module_instance=1&id=2638>; Internet; accessed 10 December 2004.

[49] Chief Information Office, 3.

[50] Achterberg.

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Chief Information Office, 3.

[56] Ibid.

[57] Grant Gross, "FBI Trying to Salvage $170 million software package," 17 January 2005; available from http://www.cio.com.au/index.php?taxid=620938001&id=283749618; Internet; accessed 22 January 2005.

[58] Ibid.

[59] Chief Information Office, 3.

[60] Kay Hammer, “Information Sharing for Homeland Security: Balancing Expectations with Technical and Cultural Capabilities,” 23 October 2002; available from <http://www.uschamber.com/…/conferencereport.pdf>; Internet; accessed 12 November 2004.

[61] Chief Information Office, 3.

[62] Alton Chua, “A Framework for Knowledge Management Implementation,” *Journal of Information & Knowledge Management,* 2, no. 1 (2003): 79.

[63] Chief Information Office, 3.

[64] Ibid.

[65] Ibid.

[66] Ibid.

[67] Office of the Secretary of Defense, Comptroller.

[68] Chief Information Office, 3.

[69] Ibid.

[70] Ibid.

[71] Ibid., 12.

[72] Chua, 82.

[73] Ibid., 83.

[74] Ibid.

[75] United States Joint Forces Command, Operational Implications of the Collaborative Information Environment (CIE), *The Joint Warfighting Center Joint Doctrine Series*; Pamphlet 5 (Washington, D.C.: U.S. Joint Forces Command, 1 June 2004), 1.

[76] Ibid.

[77] Ibid., 11.

[78] Ibid., 10.

[79] Ibid., 11.

[80] Ibid.

[81] Ibid.

[82] Rumizen, 158.

[83] Alkis Papadopoullos, “Answering the Right Questions about Search,” *EContent*. Wilton (July/Aug 2004. Vol.27, Iss. 7/8): S6 [database on-line]; available from ProQuest; accessed 21 September 2004.

[84] Ibid.

[85] Ibid.

[86] Robert David Steele, “Information Peacekeeping and Inter-Agency/Multi-National Information Sharing Proposed as Focus for 109th Congress – Intelligence Reform is Dead,” 30 November 2004; available from <http://www.news.corporate.findlaw.com/prnewswire/ 20041130/ 30nov2004143640.html>; Internet; accessed 10 December 2004.

GLOSSARY

AKM	Army Knowledge Management
C4	Command, Control, Communications and Computers
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CIO	Chief Information Operations
CM	Change Management
COP	Common Operating Picture
DA	Department of the Army
DOD	Department of Defense
DOS	Department of State
DS	Decision Superiority
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
HUMIT	Human Intelligence
IM	Information Management
IMINT	Imagery Intelligence
INS	Immigration and Naturalization Service
IS	Information Superiority
ISS	Interagency Information Sharing
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
KM	Knowledge Management
MASINT	Measurement and Signature Intelligence
NCTC	National Counterterrorism Center
NGO	Non Governmental Organization
NID	National Intelligence Director
NORAD	North American Aerospace Defense Command
NSA	National Security Agency
OSINT	Open Source Intelligence
SIGINT	Signals Intelligence
TECHINT	Technology Intelligence

BIBLIOGRAPHY

Achterberg, Maribeth. “How Culture Affects Information Sharing in an Organization.” 30 November 2001. Available from <http://www.kwork.org/White_Papers/cultural.html>. Internet. Accessed 12 November 2004.

Bergeron, Bryan. *Essentials of Knowledge Management*. Hoboken: John Wiley & Sons, 2003.

Bush, George W. “Executive Order National Counterterrorism Center.” 27 August 2004. Available from <http://www.whitehouse.gov/new/releases/2004/08/20040827-5.html>. Internet. Accessed 8 October 2004.

Bush, George W. *National Strategy for Homeland Security.* Washington, D.C.: The White House, July 2002.

Chief Information Office, United States Army. *The Army Knowledge Management Strategic Plan*, 2nd. Washington, D.C.: U.S. Government Printing Office, 2003.

Chua, Alton. “A Framework for Knowledge Management Implementation,” *Journal of Information & Knowledge Management*, 2, no. 1 (2003).

Davenport, Thomas H., and Laurence Prusak. *Working Knowledge: How Organizations Manage What They Know*. Boston, MA: Harvard Business School Press, 2000.

Fiorill, Joe. “Panel Seeks Broad Terrorism Information-Sharing Changes.” 13 December 2004. Available from <http:// www.govexec.com/dailyfed/1204/121304gsn1.htm>. Internet. Accessed 17 December 2004.

Fong, Mei. “Mind over Matter.” *Far Eastern Economic Review* (July 29, 2004, 167, Iss. 30): 39. Database on-line. Available from ProQuest. Accessed 21 September 2004.

Gross, Grant. “FBI Trying to Salvage $170 million software package,” 17 January 2005. Available from <http://www.cio.com.au/index.php?taxid=620938001&id=283749618>. Internet. Accessed 22 January 2005.

Hammer, Kay. “Information Sharing for Homeland Security: Balancing Expectations with Technical and Cultural Capabilities.” 23 October 2002. Available from <http://www. uschamber.com/…/conferencereport.pdf. Internet. Accessed 12 November 2004.

Kelley, Juris. “Overcoming Information Sharing Obstacles and Complexity.” November 2003. Available from <http://www.chm.net/docimg/wp_overcoming.pdf>. Internet. Accessed 12 November 2004.

Koenig, Michael E.D., and T. Kanti Srikantaiah, eds. *Knowledge Management, Lessons Learned, What Works and What Doesn’t.* Medford, NJ: ASSIS&T, 2004.

Lewis, James T. “Reform by Catastrophe: How the Department of Homeland Security Fails America’s Need for Real Intelligence Reform.” November 2004. Available from <http://www.american.edu/sis/students/sword/back_issues/7.pdf>. Internet. Accessed 19 December 2004.

Myers, Richard B. *National Military Strategy of the United States of America 2004.* Washington, D.C.: U.S. Government Printing Office, 2004.

The 9/11 Commission. *Final Report of the National Commission on Terrorist Attacks Upon the United States.* Washington, D.C.: U.S. Government Printing Office, 2004.

Office of the Secretary of Defense, Comptroller. “Knowledge Management.” 21 September 2004. Available from <http://www.defenselink.mil/comptroller/icenter/learn/knowledgeman.htm>. Internet. Accessed 21 September 2004.

Papadopoullos, Alkis. “Answering the Right Questions about Search.” *EContent*. Wilton (July/Aug 2004. 27, Iss. 7/8): S6 Database on-line. Available from ProQuest. Accessed 21 September 2004.

Reimer, Charles Mr HQDA DCS G-3/5/7 <charles.reimer@us.army.mil>. “9-11 Commission Report.” Electronic mail message to William T. Johnsen, Ph.D <William.Johnsen@carlisle.army.mil>, 24 September 2004.

Rumizen, Melissie Clemmons. *The Complete Idiot’s Guide to Knowledge Management.* Madison, WI: CWL Publishing Enterprises, 2002.

Sarkar, Dibya. “9/11 Report Urges Info Sharing, Biometrics.” 20 September 2004. Available from <http://www.fcw.com/fcw/articles/2004/0719/web-911-07-22-04.asp>. Internet. Accessed 20 September 2004.

Seabrook, Andrea. “Senate Approves U.S. Intelligence Overhaul.” 7 October 2004. Available from <http://www.npr.org/templates/story/story.php?storyId=4074833>. Internet. Accessed 8 October 2004.

Sequist, Larry. “Information Peacekeeping & Collective Intelligence.” 3 December 2004. Available from <http://www.oss.net/extra/news/?module_instance=1&id=2638>. Internet. Accessed 10 December 2004.

Steele, Robert David. “Information Peacekeeping and Inter-Agency/Multi-National Information Sharing Proposed as Focus for 109th Congress – Intelligence Reform is Dead.” 30 November 2004. Available from <http://www.news.corporate.findlaw.com/prnewswire/20041130/30nov2004143640.html>. Internet. Accessed 10 December 2004.

United States Joint Forces Command, Operational Implications of the Collaborative Information Environment (CIE), *The Joint Warfighting Center Joint Doctrine Series*; Pamphlet 5. Washington, D.C.: U.S. Joint Forces Command, 1 June 2004.